CLAIMS

1. A system for preventing theft or misuse of a computer system, the system comprising:

a computer system having a device;

an agent embedded in the device that, when authorized, enables operation of the device and that, when not authorized, disables operation of the device; and

a server coupled to the embedded agent that, by exchanging a number of messages with the embedded agent that together compose a handshake operation, authorizes the embedded agent to enable operation of the device.

2. The system of claim 1 wherein the device contains a logic circuit and the embedded agent is implemented as a logic circuit within the logic circuit of the device.

3. The system of claim 1 wherein the device transmits and receives data and control signals via a bus and wherein the embedded agent intercepts the data and control signals transmitted to the device prior to reception by the device and intercepts the data and control signals transmitted from the device prior to transmission of the data and control signals to the bus.

4. The system of claim 3 wherein the embedded agent enables the device by passing the data and control signals intercepted by the embedded agent to and from the device and wherein the embedded agent disables the device by not passing the data and control signals intercepted by the embedded agent to and from the device.

5. The system of claim 4 wherein the embedded agent is embedded in a disk drive and wherein, when authorized by the remote server, the embedded agent encrypts all intercepted data before passing the data to the disk for storage and decrypts all data intercepted from the disk drive before passing the data to the bus.

6. The system of claim 5 wherein the server continuously authorizes the embedded agent by undertaking handshake operations and wherein, when the coupling between the server and the embedded agent is interrupted or broken so that the embedded agent cannot receive additional messages from the server, the embedded agent disables the device by preventing access to the disk drive via the disk drive and by not providing decryption of the encrypted data stored on the disk drive, thereby disabling the computer system and preventing use of the computer system.

7. The system of claim 1 wherein the handshake operation comprises:

an authorization message sent from the server to the embedded agent;

following reception of the authorization message by the embedded agent, a confirm authorization message sent from the embedded agent to the server; and

following reception of the confirm authorization message by the server, completion message sent from the server to the embedded agent.

8. The system of claim 7 wherein the server authorizes the embedded agent to enable operation of the device for a certain period of time by including in the completion message the period of time for which the server authorizes operation of the device.

9. The system of claim 8 wherein the embedded agent includes a timer that is set to expire prior to expiration of the period of time of authorization received by the embedded agent in a completion message and wherein, when the timer expires, the embedded agent sends a solicitation message to the server requesting that the server undertake a handshake operation in order that the embedded agent receives an additional authorization period from the remote server to enable continuous operation of the device.

10. The system of claim 9 wherein the server repeatedly undertakes a handshake operation prior to expiration of the current period of time for which the embedded agent

is authorized to enable operation of the device so that operation of the device is not disabled during the time that the computer system is powered on and the embedded agent is coupled to the server.

11. The system of claim 10 wherein, when the device is powered on, the timer is set to a period of time sufficient for the embedded device to request a handshake operation by sending a solicitation message to the remote server and sufficient for completion of the handshake operation and wherein the embedded agent is authorized to enable operation of the device until expiration of the timer, after which the embedded agent disables the device.

12. The system of claim 11 wherein the embedded agent maintains a current password and a previous password, wherein the server maintains a current agent password and a previous agent password that correspond to the current password and previous password maintained by the embedded agent following detection of the embedded agent by receiving a solicitation from the embedded agent that includes the embedded agent's current and previous passwords; wherein the server generates a new password for the embedded agent when the server undertakes a handshake operation and includes the new password in the authorization message; wherein the embedded agent includes the new password received from the server in the authorization message as well as the current password maintained by the embedded agent in the confirm authorization message; wherein the server, upon reception of the confirm authorization message, replaces the previous agent password with the current agent password and replaces the current agent password with the new password; and wherein, upon reception of the completion message, the embedded agent replaces the previous password with current password and replaces the current password with the new password.

13. The system of claim 12 wherein the embedded agent is constructed to maintain a special initial password as both the current password and the previous password so that

the server can detect when the embedded agent sends a solicitation message to the remote server for the first time.

14. The system of claim 13 wherein, when a handshake operation fails, the server can synchronize the current agent password and previous agent password maintained by the server with the current and previous passwords maintained by the embedded agent by receiving from the embedded agent a solicitation message that contains the current and previous passwords maintained by the embedded agent.

15. The system of claim 14 wherein the server continuously authorizes the embedded agent by undertaking handshake operations and wherein, when the coupling between the remote server and the embedded agent is interrupted or broken so that the embedded agent cannot receive additional messages from the server, the embedded agent disables the device thereby disabling the computer system and preventing use of the computer system.

16. The system of claim 15, further including a client component that receives messages from the server and forwards those messages to the embedded agent and that receives messages from the embedded agent and forwards those messages to the server.

17. The system of claim 16 wherein embedded agents are embedded within several device within the computer system and wherein the client component receives messages from the embedded agents and forwards those messages to the server and wherein the client component receives messages from the server and distributes those messages to the embedded agents.

18. The system of claim 1 wherein embedded agents are embedded in additional components of the computer system including a CPU and memory devices, and wherein embedded agents are implemented as one of hardware logic circuits, firmware routines,

and software routines that run within the device or component within which the embedded agents are embedded.

19. A method for enabling and disabling operation of a component of a system, the method comprising:

embedding an agent within the component;

establishing a communications link between the embedded agent and a server; and

when the component is to be enabled, exchanging a number of messages between the server and the embedded agent that together compose a handshake operation that results in authorization of the embedded agent to enable operation of the component for a period of time.

20. The method of claim 19, further including:

when the last period of time for which the embedded agent has been authorized to enable operation of the component will expire within a period of time sufficient for sending a second solicitation message and for completing a handshake operation, sending a solicitation message from the embedded agent to the server in order request a handshake operation.

21. The method of claim 19, further including:

including a timer in the embedded agent;

when the component is powered-up or initialized for operation, setting the timer for a period of time sufficient for the embedded agent to establish the communications link with the server, to send a solicitation message to the server requesting a handshake operation, and to complete the handshake operation;

after establishing a communications link between the embedded agent and the server, sending a solicitation message from the embedded agent to the server requesting a handshake operation;

when the handshake operation is completed, resetting the timer to expire prior to expiration of the period of time for which the embedded agent is authorized to enable operation of the component to allow the embedded agent sufficient time to send a second solicitation message to the server requesting a second handshake operation and to complete a second handshake operation prior to expiration of the period of time for which the embedded agent is authorized to enable operation of the component;

when the timer expires prior to expiration of the period of time for which the embedded agent is authorized to enable operation of the component, sending the second solicitation message from the embedded agent to the server in order to request the second handshake operation and resetting the timer to expire after a period of time sufficient to send a third solicitation message to the server requesting a third handshake operation and to complete the third handshake operation; and

when the timer expires following expiration of the period of time for which the embedded agent is authorized to enable operation of the component, disabling the component.

22. The method of claim 19, further including:

after establishing a communications link between the embedded agent and the server, sending a solicitation message from the embedded agent to the server requesting a handshake operation;

when the server receives the solicitation message from the embedded agent, undertaking, by the server, a handshake operation in order to authorize the embedded agent.

23. The method of claim 22 wherein the handshake operation further includes:

sending an authorization message from the server to the embedded agent;

receiving the authorization message by the embedded agent and returning by the embedded agent a confirm authorization message to the server; and receiving the confirm authorization message by the server and returning by the server an completion message to the embedded agent.

24. The method of claim 23, further including:

maintaining a current password and a previous password within the embedded agent; and

maintaining a current agent password and a previous agent password within the sever.

25. The method of claim 24, further including:

prior to sending the authorization message by the server, generating a new password, storing the new password within the server, and including the new password in the authorization message;

upon receiving the authorization message by the embedded agent, storing the new password within the embedded agent and including both the new password and the maintained current password in the confirm authorization message that the embedded agent returns to the server;

upon receiving the confirm authorization message by the server,

comparing the new password and the current password contained in the confirm authorization message with the new password stored within the server and the current agent password maintained within the server; and

when the new password contained in the confirm authorization message is identical to the new password stored within the server and the current password contained in the confirm authorization message is identical to the current agent password maintained within the server,

setting the previous agent password maintained within the server to the current agent password maintained within the server; and

setting the current agent password maintained within the server to the new password stored within the server; and

upon receiving the completion message by the embedded agent, setting the previous password maintained within the embedded agent to the current password maintained within the embedded agent, and

setting the current password maintained within the embedded agent to the new password stored within the embedded agent.

26. The method of claim 25, further including:

constructing the embedded agent to maintain initial passwords as the current and previous passwords.

27. The method of claim 24, further including:

maintaining a linear feedback mechanism within the server that is initialized with a seed value and that successively and deterministically generates new passwords; and

maintaining a linear feedback mechanism within the embedded agent that is initialized with the seed value and that successively and deterministically generates the same new passwords that are generated by the linear feedback mechanism within the server.

28. The method of claim 27, further including:

prior to sending the authorization message from the server, generating by the server a new password and including a value related to the new password in the authorization message; and

upon receiving the authorization message by the embedded agent,

generating a new password within the embedded agent,

comparing a value related to the newly generated password within the embedded agent with the value related to the new password contained in the authorization message, and

when the value related to the newly generated password within the embedded agent is identical with the value related to the new password contained in the authorization message, sending the confirm authorization message from the embedded agent to the server.

29. The method of claim 27, further including exchanging the seed value between the server and the embedded agent when the embedded agent first establishes the communications link with the server.

30. The method of claim 19 wherein the component of the system is a component of a computer system and wherein the embedded agent is embedded in the component of the computer system, and further including:

running a software program that implements the server on a remote computer to provide a remote server; and

enabling operation of the computer system that contains the component by the remote server authorizing the embedded agent to enable operation of the component.

31. The method of claim 30, further including disabling the computer system causing the embedded agent to disable the component.

32. The method of claim 30 wherein the embedded agent is a software program within a controller software program that controls the component, the embedded agent communicating with the remote server via internal buses within the computer system and via external communication media between the computer system and the remote server, including at least one of local area networks, wide area networks, and combinations of local area networks and wide area networks.

33. The method of claim 30 wherein the embedded agent is a logic circuit within an application specific integrated circuit that implements the controller of a disk drive; and further including:

intercepting by the embedded agent all data transfers to the disk drive and, when authorized, encrypting the data prior to passing the data to the disk drive; and

intercepting by the embedded agent all data transfers from the disk drive and, when authorized, decrypting the previously encrypted data prior to passing the data from the disk drive.

34. The method of claim 33, further including disabling and enabling specific data stored on the disk drive by including an identification of the data to be enabled and disabled in an authorization message that is sent from the server to the embedded agent.

35. The method of claim 30 wherein the component exchanges data and messages with the computer system, and further including:

intercepting by the embedded agent all messages and data exchanged between the component and the computer system;

when the embedded agent is authorized, enabling the component by passing messages and data from the computer system to the component and by passing messages and data from the component to the computer system; and

when the embedded agent is not authorized, disabling the component by not passing messages and data from the computer system to the component and by not passing messages and data from the component to the computer system.

36. The method of claim 30, further including protecting the computer system from theft or misuse by requiring the remote server to repeatedly authorize the embedded agent.

37. The method of claim 30, further including selectively enabling and disabling multiple components of the computer system by embedding a plurality of agents within the multiple components and selectively authorizing the multiple components from the remote server.

38. The method of claim 37, further including exchanging additional information between the plurality of embedded agents and the remote server, including information concerning workloads placed on the components in which the embedded agents are embedded, in order to allow the computer system to enable and disable components to adjust operation of the components to operate more efficiently based upon the workload information.

39. The method of claim 37, further including enabling components of the computer system in response to receiving payments for operation of the components.

40. The method of claim 19 wherein the component of the system is an executing software program, wherein the system is a computer system, and wherein the embedded agent is implemented as a software subcomponent of the software program, the method further including:

running a software program that implements the server on a remote computer to provide a remote server; and

enabling execution of the software program by authorizing the embedded agent subcomponent of the software program.

41. The method of claim 19, further including controlling use of a firearm by embedding an agent into a component of the firearm required to discharge the firearm.

42. The method of claim 19, further including controlling use of a firearm by embedding an agent into a component of the firearm required to load the firearm.

43. The method of claim 19, further including diagnosing a powered-down or disabled component by detecting when the embedded agent within the component does not respond to authorization messages sent from the server.

44. A control system for controlling operation of components within a multi-component system, the control system comprising:

an agent embedded in a component of the multi-component system that, when authorized, enables operation of the component and that, when not authorized, disables operation of the device; and

a server coupled to the embedded agent that, by exchanging a number of messages with the embedded agent that together compose a handshake operation, authorizes the embedded agent to enable operation of the component.

45. The control system of claim 44 wherein the multi-component system is a computer system, wherein the embedded agent is embedded within a disk drive of the computer system, wherein the embedded agent selectively enables and disables reading and transmission of software programs stored on the disk drive to other components of the computer system, and wherein the control system implements a pay per use control system that enables software programs pre-installed in the computer system when payment is received for use of the software programs.

46. The control system of claim 44 wherein the multi-component system is a firearm, wherein the embedded agent is embedded within the firing mechanism of the firearm, and wherein the control system implements a gun control system that selectively enables use of the firearm.

47. The control system of claim 44 wherein the server monitors successful handshake operations in order to detect interruption or loss of operation of the component within which the embedded agent is embedded, thereby diagnosing interruption or loss of operation of the component.

48. The control system of claim 44 wherein the server exchanges additional informational messages with the embedded agent that enables the server to instruct the embedded agent to adjust and modify operational characteristics of the device in which the embedded agent is embedded.

49. A method for enabling the operation of a system upon receiving, by the system, a valid identifier, the method comprising:

embedding an agent within a component of the system that can receive an identifier and that can enable operation of the system;

establishing a communications link between the embedded agent and a server;

exchanging a number of messages between the embedded agent and the server that results in authorization of the embedded agent to subsequently enable operation of the system upon receiving a valid identifier; and

when an identifier is received by the component of the system,

obtaining the received identifier from the component of the system by the embedded agent;

exchanging a number of messages between the embedded agent and the server that transfer the received identifier from the embedded agent to the server and that results in the embedded agent receiving authorization from the server to enable operation of the system when the server determines that the identifier is valid and that results in the embedded agent not receiving authorization from the server to enable operation of the system when the server determines that the identifier is invalid; and

enabling operation of the system by the embedded agent upon receiving authorization from the server to enable operation of the system.

50. The method of claim 49 wherein the embedded agent is linked to the server via the Internet.

51. The method of claim 49 wherein the system is a computer system, wherein the identifier is included within a software computer program, and wherein the embedded agent is authorized by the server to enable the computer system to run the software computer program when the server determines that the identifier is valid.

52. The method of claim 49 wherein the system is an entertainment system that reads entertainment information from a medium and presents the entertainment information, wherein the identifier is included in the medium, and wherein the embedded agent is authorized by the server to enable the entertainment system to read the entertainment information from the medium and present the read entertainment information when the server determines that the identifier is valid.

53. The method of claim 52 wherein the entertainment system reads audio information from the medium and presents the audio information by converting the audio information into an audio signal, amplifying the audio signal, and broadcasting the audio signal through one or more loudspeakers.

54. The method of claim 53 wherein the medium is DVD disc.

55. The method of claim 53 wherein the medium is a compact disk.

56. The method of claim 53 wherein the medium is a magnetic tape.

57. The method of claim 53 wherein the medium is a broadcast electronic signal.

58. The method of claim 52 wherein the entertainment system reads video information from the medium and presents the video information by converting the video information into a visual display signal and broadcasting visual display signal through one or more visual display devices.

59. The method of claim 58 wherein the medium is DVD disc.

60. The method of claim 58 wherein the medium is a magnetic tape.

61. The method of claim 58 wherein the medium is a broadcast electronic signal.

62. The method of claim 49 wherein the system may be occupied by a human and is entered by a door, wherein the identifier is included in an electronic key, and wherein the embedded agent is authorized by the server to enable a door lock to open when the server determines that the identifier is valid.

63. The method of claim 62 wherein the system is a residence.

64. The method of claim 62 wherein the system is an automobile or truck.

65. The method of claim 62 wherein the system is an airplane.

66. The method of claim 62 wherein the system is a boat.

67. The method of claim 62 wherein the system is a tractor.

68. The method of claim 49 further including:

periodically reacquiring the identifier by the embedded agent, exchanging a number of messages between the embedded agent and the server, and, when the server determines that the reacquired identifier is valid, re-enabling operation of the system by the embedded agent upon receiving authorization from the server to enable operation of the system; and when the server determines that the system has been misappropriated or is being misused, not sending to the embedded agent and further authorizations from the server to enable operation of the system so that the system becomes disabled.

69. The method of claim 68 wherein the system is an automobile or truck.

70. The method of claim 68 wherein the system is an airplane.

71. The method of claim 68 wherein the system is a boat.

72. The method of claim 68 wherein the system is a tractor.

73. The method of claim 49 wherein the system is a transaction system that accepts currency, wherein the identifier is embedded within the currency, and wherein the embedded agent is authorized by the server to accept the currency during a transaction when the server determines that the identifier is valid, and wherein the server monitors invalid identifiers in order to detect and signal fraudulent transactions and counterfeited currency.